Experimental realisation of quantum oblivious transfer

Ryan Amiri[1], Robert Stárek[2], Michal Mičuda[2], Ladislav Mišta[2], Jr., Miloslav Dušek[2], Petros Wallden[3], and Erika Andersson[1]

[1] SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom

[2] Department of Optics, Palacký University, Olomouc, Czech Republic

[3] LFCS, School of Informatics, University of Edinburgh,10 Crichton Street, Edinburgh EH8 9AB, United Kingdom

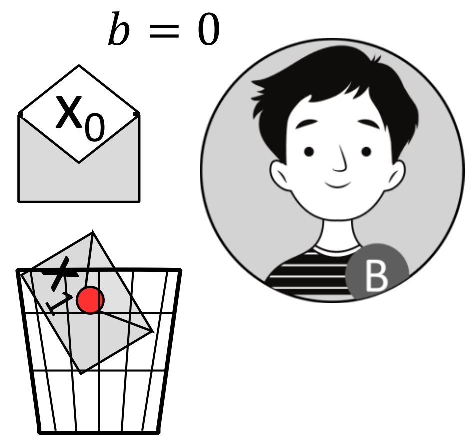
QCrypt 2020

arXiv:2007.04712

Oblivious transfer – basic idea

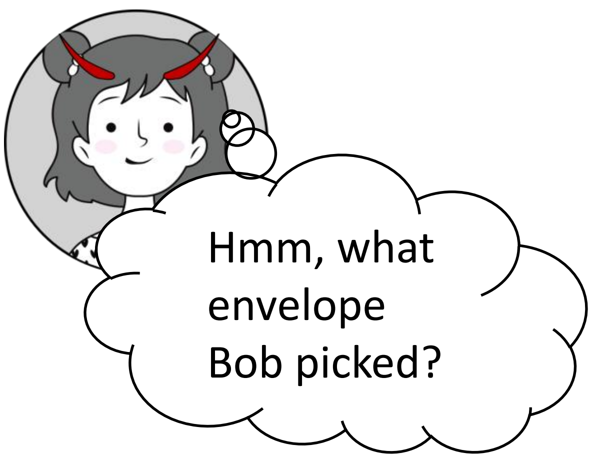
- Alice picks bits, x_0 and x_1. Bob picks bit b.
- Alice and Bob communicate.

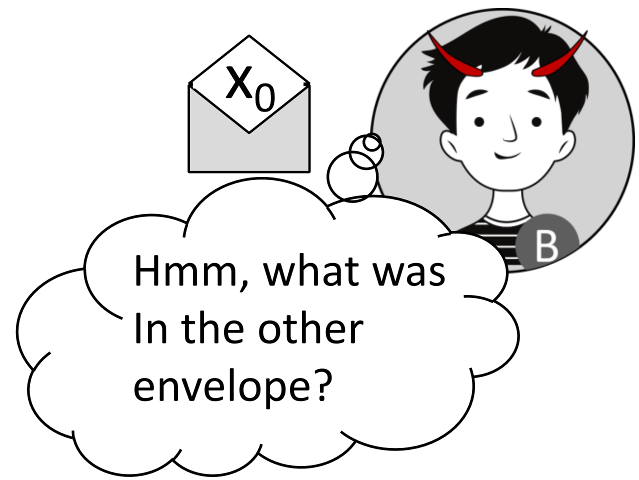
Oblivious transfer – basic idea



- Alice picks bits, x_0 and x_1. Bob picks bit b.
- Alice and Bob communicate. Bob receives x_b.

Oblivious transfer – basic idea





- Alice picks bits, x_0 and x_1. Bob picks bit b.
- Alice and Bob communicate. Bob receives x_b.
- Alice does not know b. She can guess it at most with probability $A_{OT} = ½ + \varepsilon$.
- Bob does not know $x_{\bar{b}}$. He can guess it at most with probability $B_{OT} = ½ + \varepsilon$.

Oblivious transfer - context

- Cryptographic primitive
- Applications
  - Secure multiparty computation
  - *E-voting*
  - *Signatures*
- Similar tasks
  - Bit commitment
  - Coin flipping
  - Both implementable with OT

- Classically theoretically insecure (without computational assumptions)
- Perfect implementation is impossible

- M. Blum, Three applications of the oblivious transfer, University of California, Berkeley, CA, USA, 1981
- S. Even, et al., A randomized protocol for signing contracts, Communications of the ACM (1985)
- O. Goldreich and R. Vainish, How to Solve any Protocol Problem - An Efficiency Improvement, CRYPTO'87, p. 73-86 (1987)
- J. Kilian, Founding cryptography on oblivious transfer, STOC'88, p. 20-31 (1988)

Quantum oblivious transfer (OT)

- Interesting features of quantum physics
  - Inherent randomness
  - Strong correlations
  - Quantum measurements
  - No-cloning theorem
- QKD – great success
- Quantum weak coin flipping - arbitrarily secure
- Quantum bit commitment - limited cheating
- <u>What about cheating bounds for oblivious transfer?</u>

- C. Mochon, Quantum weak coin flipping with arbitrarily small bias, arXiv:0711.4114 (2007).
- A. Chailloux and I. Kerenidis, Optimal Bounds for Quantum Bit Commitment, FOCS'11, p. 354-362 (2011).
- C. H. Bennet and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, The. Comput. Sci. 100, p. 7-11 (2014)
- H.-K. Lo and H. F. Chau, Is Quantum Bit Commitment Really Possible?, Phys. Rev. Lett. 78, 3410 (1997)
- D. Mayers, Unconditionally Secure Quantum Bit Commitment is Impossible, Phys. Rev. Lett. 78, 3413 (1997)

1-2 quantum OT

- Formal definition …
- Cheating probability
  $p_c = \max\{A_{OT}, B_{OT}\}$
- What is the achievable cheating probability?

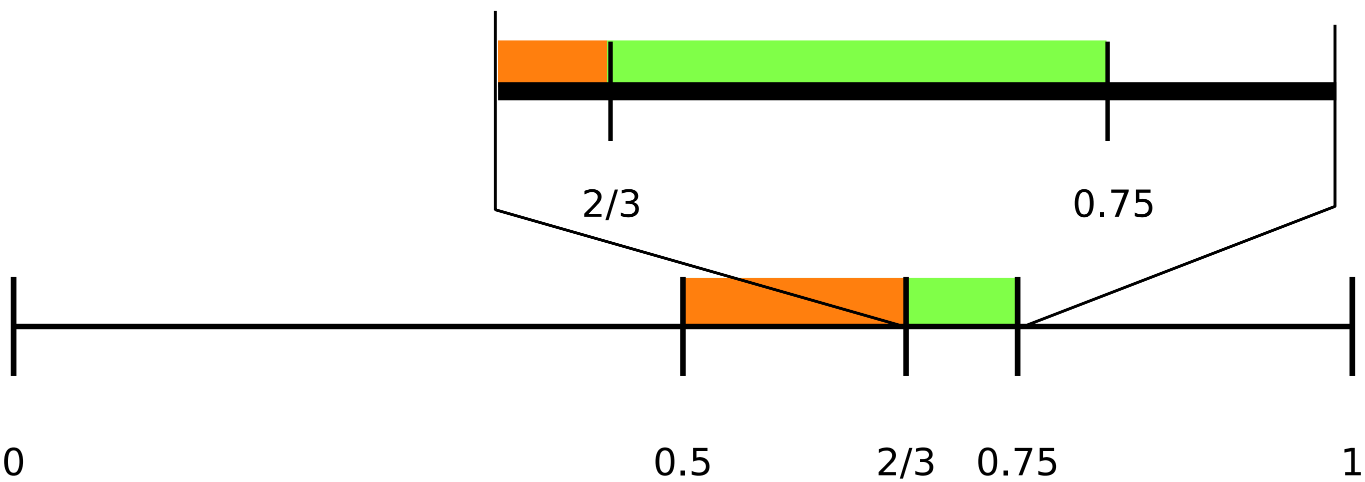
Definition 1. *A 1-2 quantum OT protocol is a protocol between two parties, Alice and Bob, such that*

- *Alice has inputs* $x_0, x_1 \in \{0,1\}$ *and Bob has input* $b \in \{0,1\}$. *At the beginning of the protocol, Alice has no information about* b *and Bob has no information about* (x_0, x_1).
- *At the end of the protocol, Bob outputs* y *or Abort and Alice can either Abort or not.*
- *If Alice and Bob are honest, they never Abort,* $y = x_b$, *Alice has no information about* b *and Bob has no information about* $x_{b \oplus 1}$.
- $A_{OT} := \sup\{\Pr[\textit{Alice correctly guesses } b \wedge \textit{Bob does not Abort}]\} = \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob correctly guesses } (x_0, x_1) \wedge \textit{Alice does not Abort}]\} = \frac{1}{2} + \epsilon_B$

- A. Chailloux, et al., Lower Bounds for Quantum Oblivious Transfer, Quant. Inf. Comput. 13, p. 158-177 (2013).

1-2 quantum OT

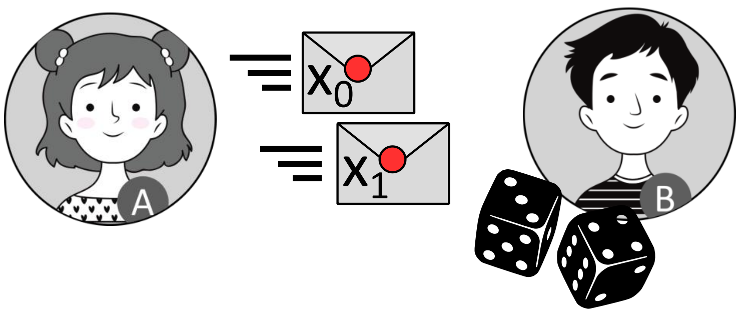
- Formal definition …
- Cheating probability
  $p_c = \max\{A_{OT}, B_{OT}\}$
- What is the achievable cheating probability?



- [A. Chailloux, et al., Lower Bounds for Quantum Oblivious Transfer, Quant. Inf. Comput. 13, p. 158-177 (2013).]

1-2 semi-random quantum OT

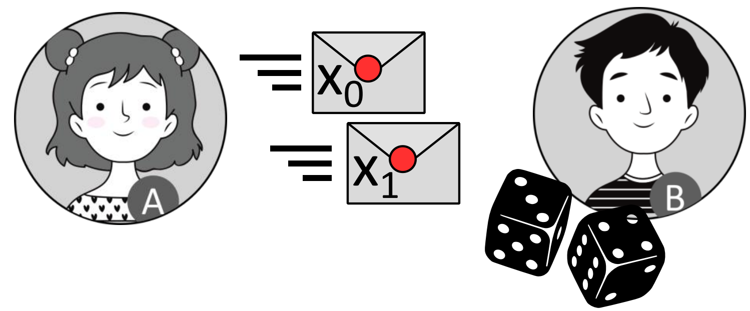
- Formal definition …



Definition 4. *1-2 quantum Semi-random OT, or simply Semi-random OT, is a protocol between two parties, Alice and Bob, such that*

- *Alice chooses two input bits* $(x_0, x_1) \in \{0,1\}$ *or Abort.*
- *Bob outputs two bits* (c, y) *or Abort.*
- *If Alice and Bob are honest, they never Abort,* $y = x_c$*, Alice has no information about* c *and Bob has no information on* $x_{c\oplus 1}$*. Further,* x_0, x_1 *and* c *are uniformly random bits* [9]*.*
- $A_{OT} := \sup\{\Pr[\textit{Alice correctly guesses } c \wedge \textit{Bob does not Abort}]\} = \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob correctly guesses } (x_0, x_1) \wedge \textit{Alice does not Abort}]\} = \frac{1}{2} + \epsilon_B$

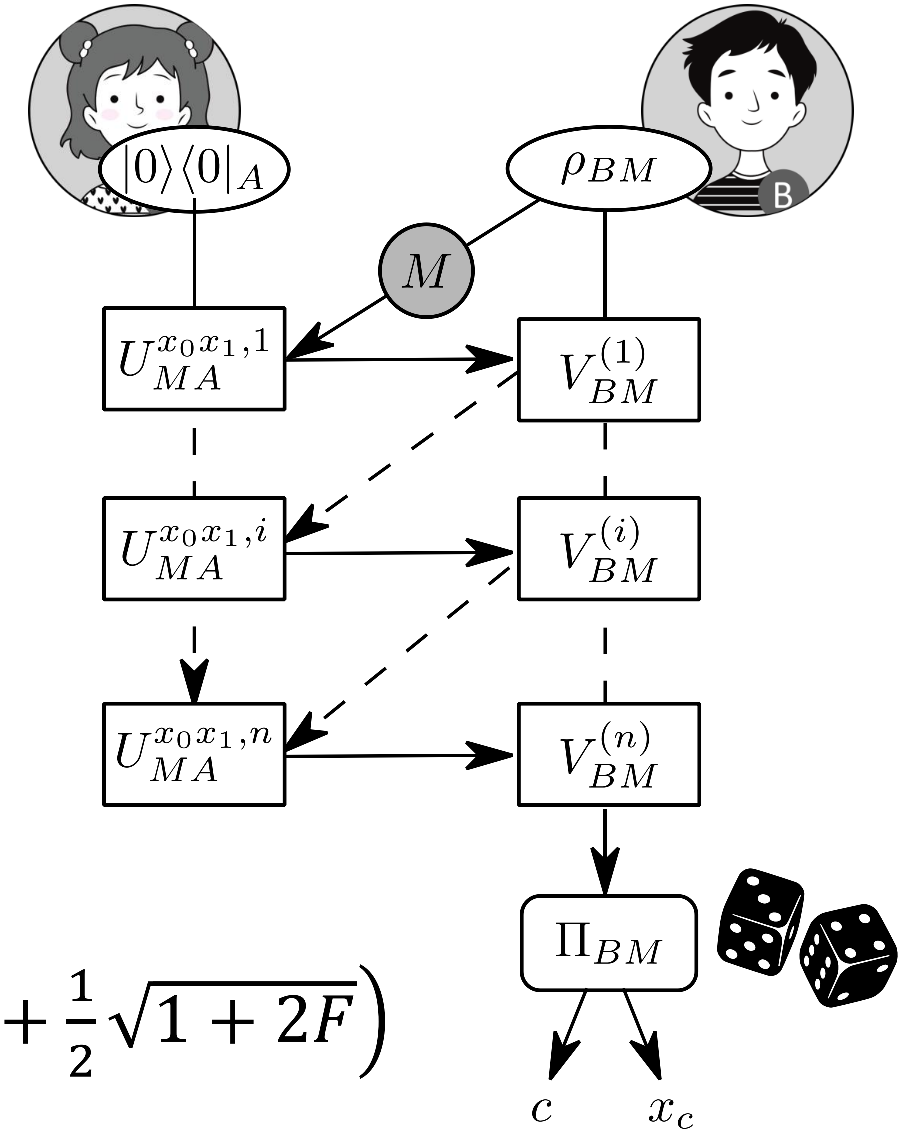
1-2 semi-random quantum OT



- Equivalent to OT up to classical processing
- Security of generic protocol?
- Specific protocol is introduced

1-2 semi-random quantum OT

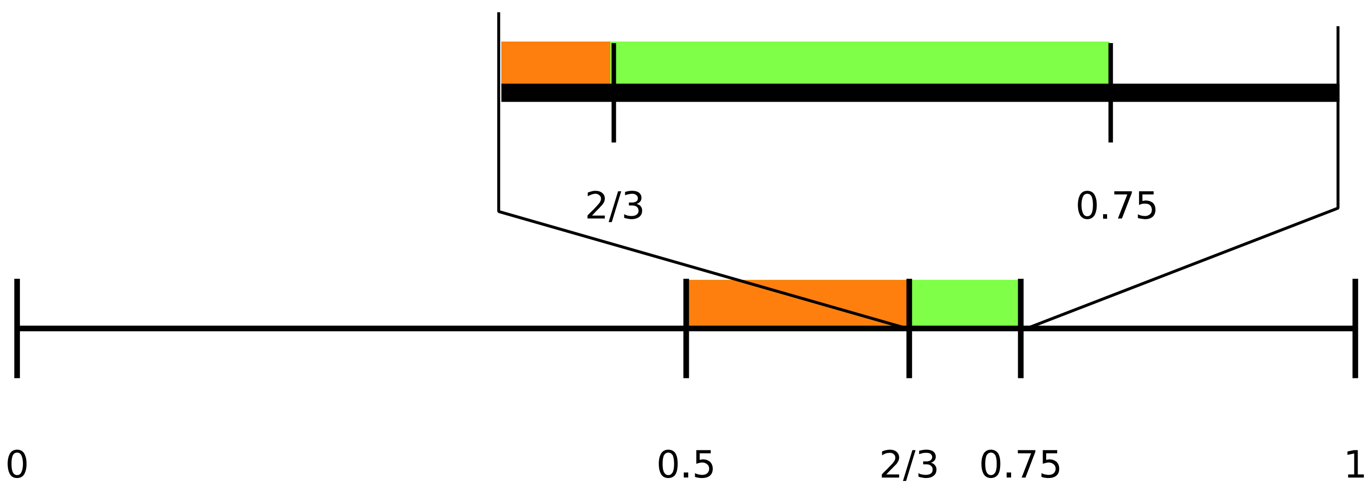
- Equivalent to OT up to classical processing
- Most general protocol
- Security expressed in terms of respective protocol state fidelities F (honest)
- Lower bound is set.



- $A_{OT} \geq \frac{1}{2}(1+F)$
- $B_{OT} \geq 1-F$
- $B_{OT}^{PS} = \frac{1}{4}\left(1 + \frac{1}{2}\sqrt{1-2F} + \frac{1}{2}\sqrt{1+2F}\right)$

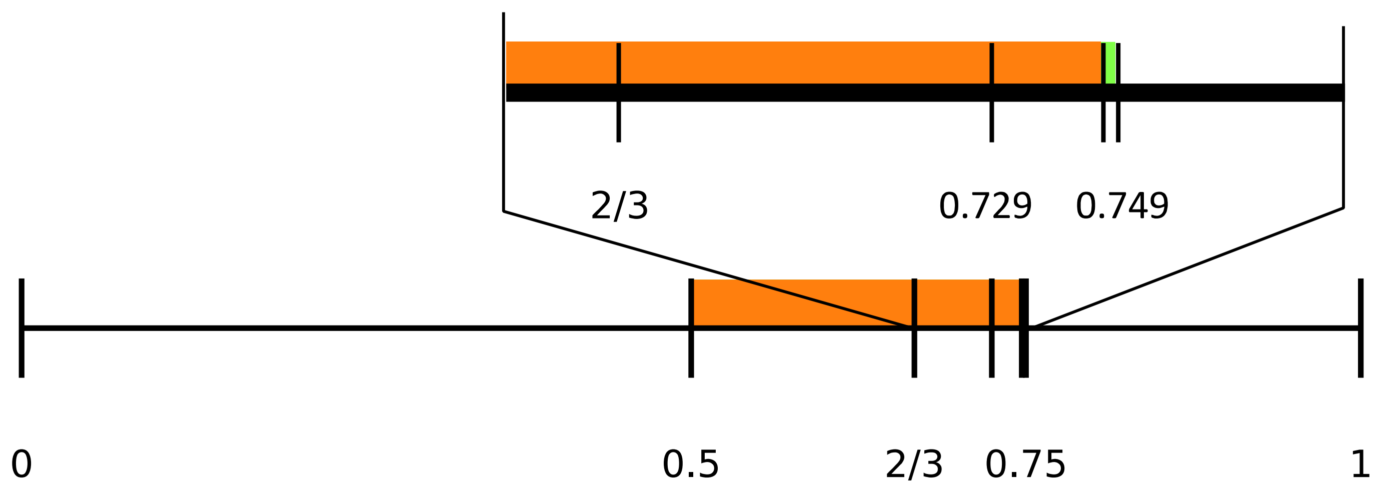
1-2 semi-random quantum OT

- Tightening the security bounds (for symmetric and pure states)
- $A_{OT} \geq \frac{1}{2}(1+F)$
- $B_{OT} \geq 1-F$
- $B_{OT}^{PS} = \frac{1}{4}\left(1+ \frac{1}{2}\sqrt{1-2F} + \frac{1}{2}\sqrt{1+2F}\right)$
- $\min_F(\max\{A_{OT}, B_{OT}\}) \approx 0.749$

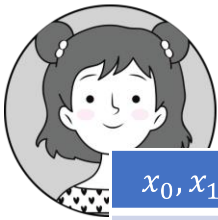


1-2 semi-random quantum OT

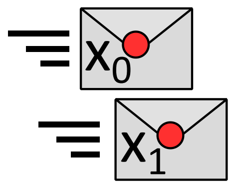
- Tightening the security bounds (for symmetric and pure states)
- $A_{OT} \geq \frac{1}{2}(1 + F)$
- $B_{OT} \geq 1 - F$
- $B_{OT}^{PS} = \frac{1}{4}\left(1 + \frac{1}{2}\sqrt{1-2F} + \frac{1}{2}\sqrt{1+2F}\right)$
- $\min_F(\max\{A_{OT}, B_{OT}\}) \approx 0.749$



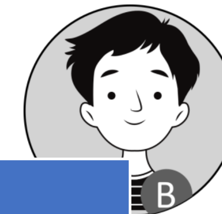
A semi-random OT protocol based on unambiguous measurements



x_0, x_1	encoded qubits
0,0	$\|00\rangle$
0,1	$\|++\rangle$
1,0	$\|--\rangle$
1,1	$\|11\rangle$



classical state declaration



Mode	Bob's meas. basis
Transfer	ZX
Test, Alice declares 0,1 or 1,0	XX
Test, Alice declares 0,0 or 1,1	ZZ

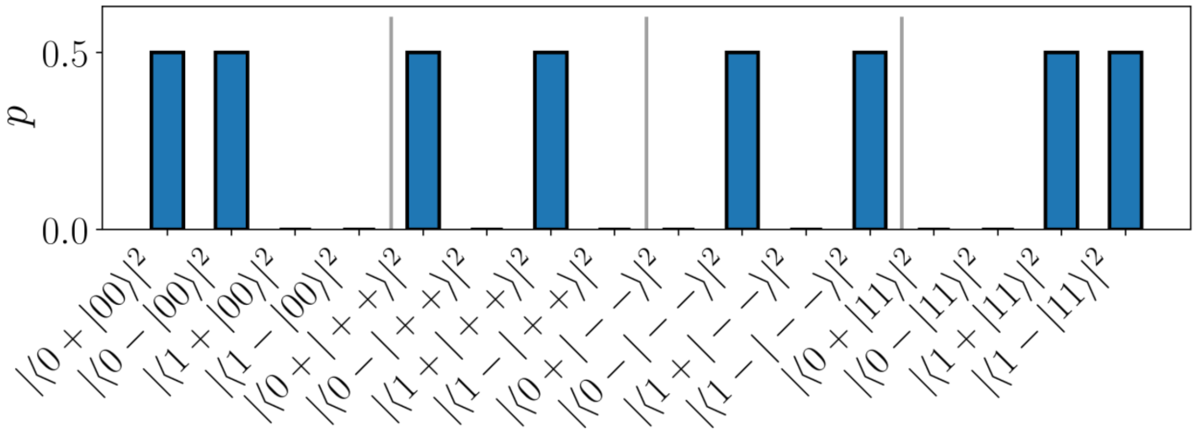
abort

c, x_c

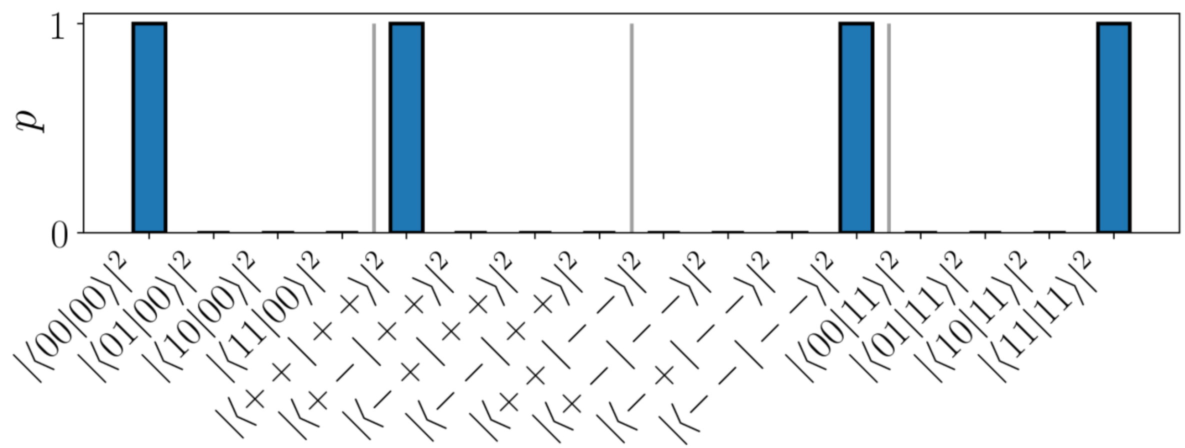
- $A_{OT} = \frac{3}{4}$
- $B_{OT} \approx 0.729$

Bob’s detection - principle

Bob’s outcome probabilities – transfer measurement



Bob’s outcome probabilities – test measurement

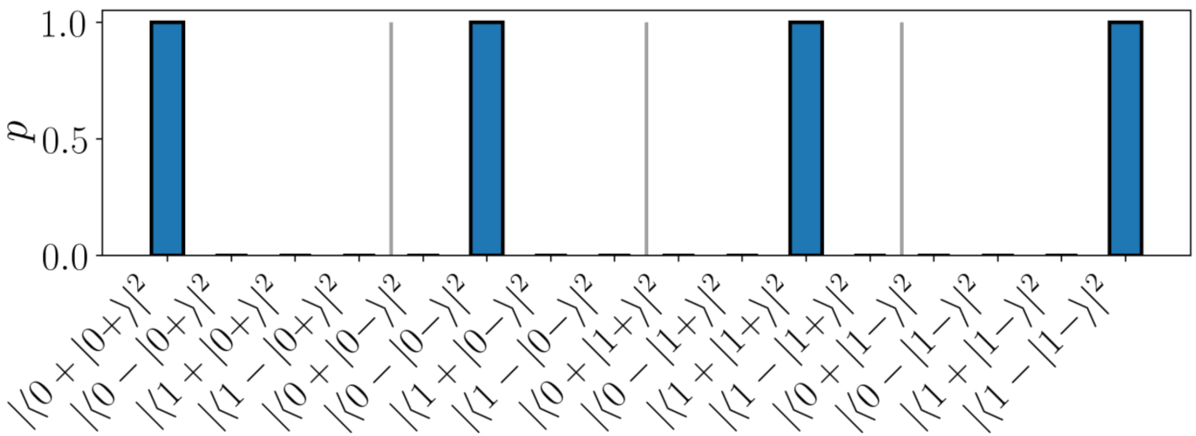


Bob’s decoding table

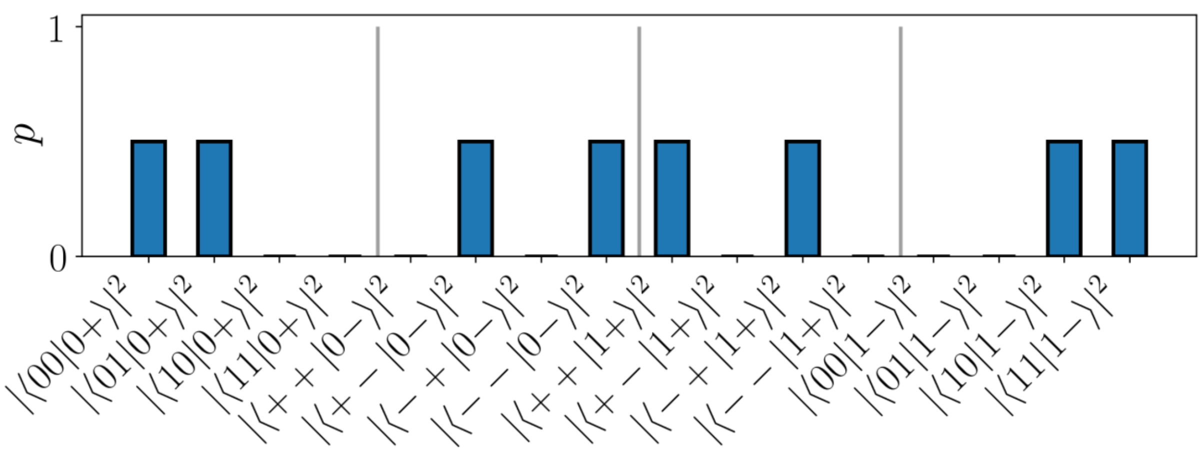
Outcome	c	x_c
0,+	0	0
0,-	1	0
1,+	1	1
1,-	0	1

Bob’s detection

Bob’s outcome probabilities – transfer measurement



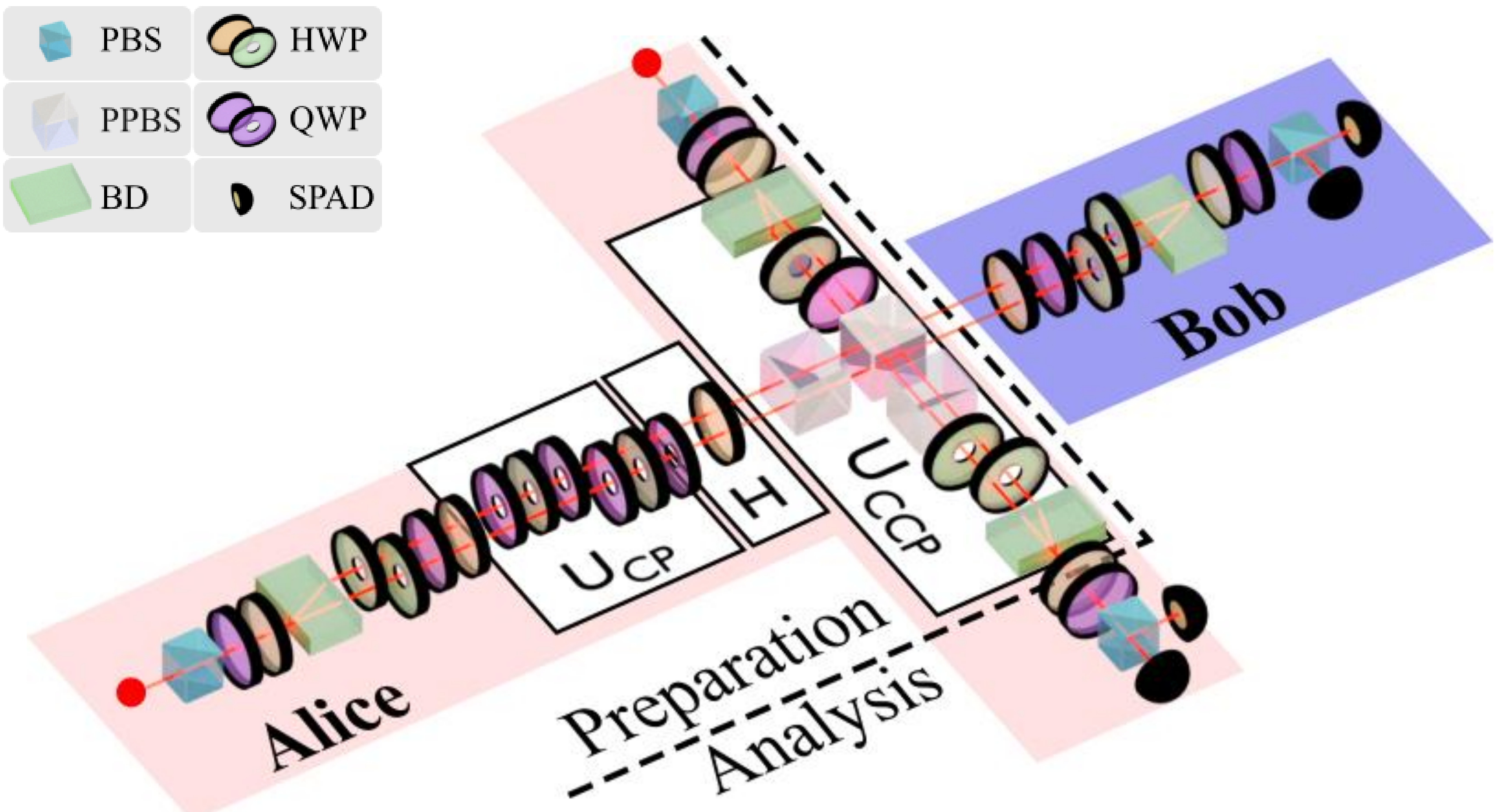
Bob’s outcome probabilities – test measurement



Alice is *naively* cheating.

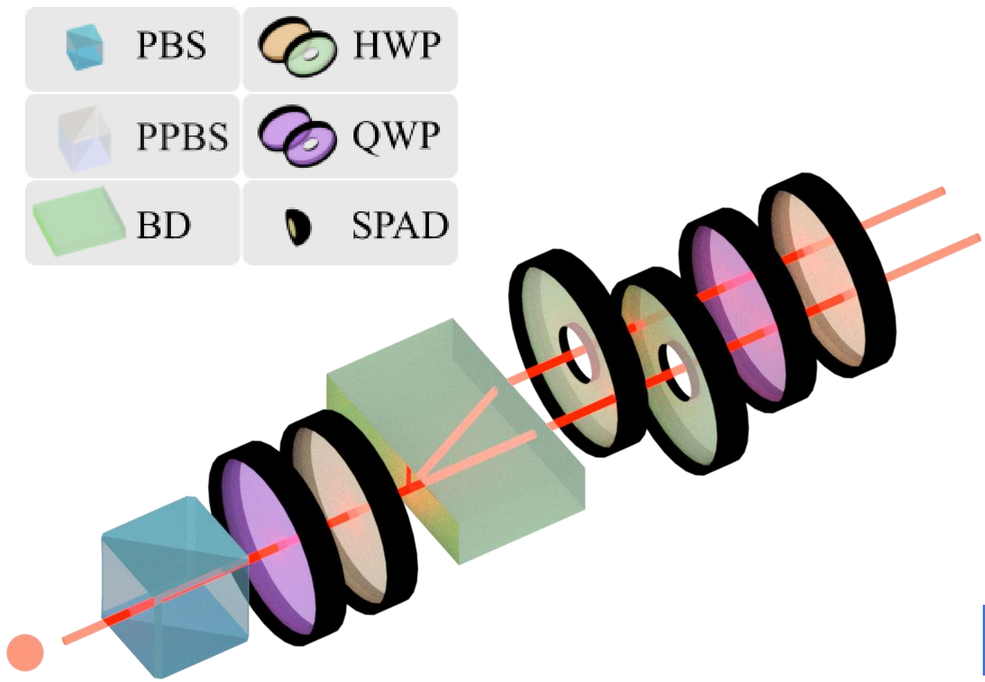
- Encoding states are eigenkets of Bob’s projector.
- Alice knows Bob’s *c.*
- *n* rounds of communication.
- Test performed $\sqrt{n}$ times.
- Protocol aborts with $p = 1 - 2^{-n/2}$.

Photonic proof-of-principle



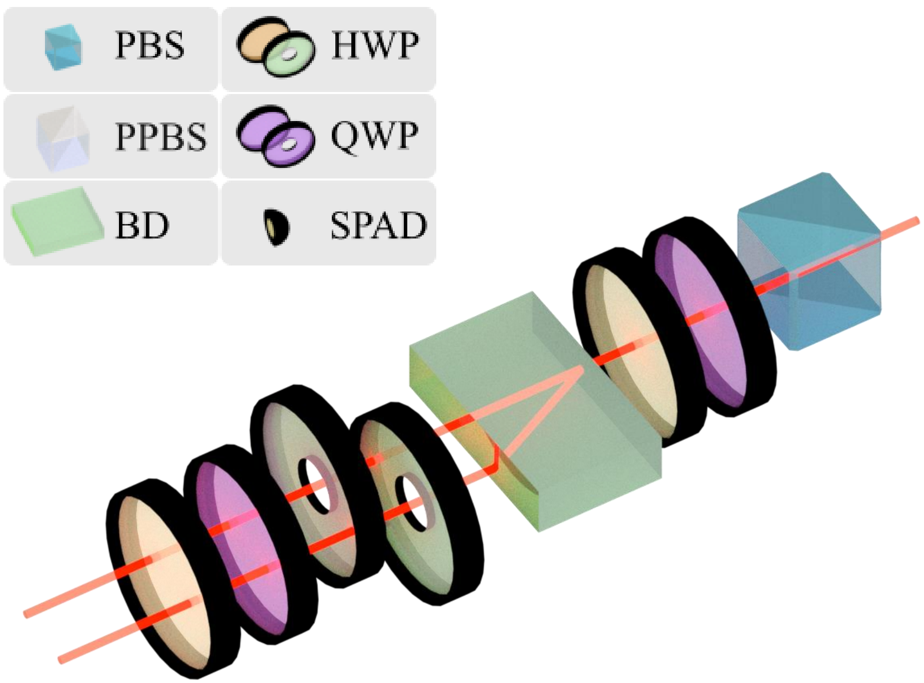
Qubit encoding

- SPDC source
- Path and polarization encoding
- One photon – two qubits
- In Alice cheating strategy we entangle the signal photon with the idler
- Transcoding into different degrees of freedom is in principle possible



x_0, x_1	encoded qubits
0,0	$\mid\uparrow H\rangle$
0,1	$\mid + D\rangle$
1,0	$\mid - A\rangle$
1,1	$\mid\downarrow V\rangle$

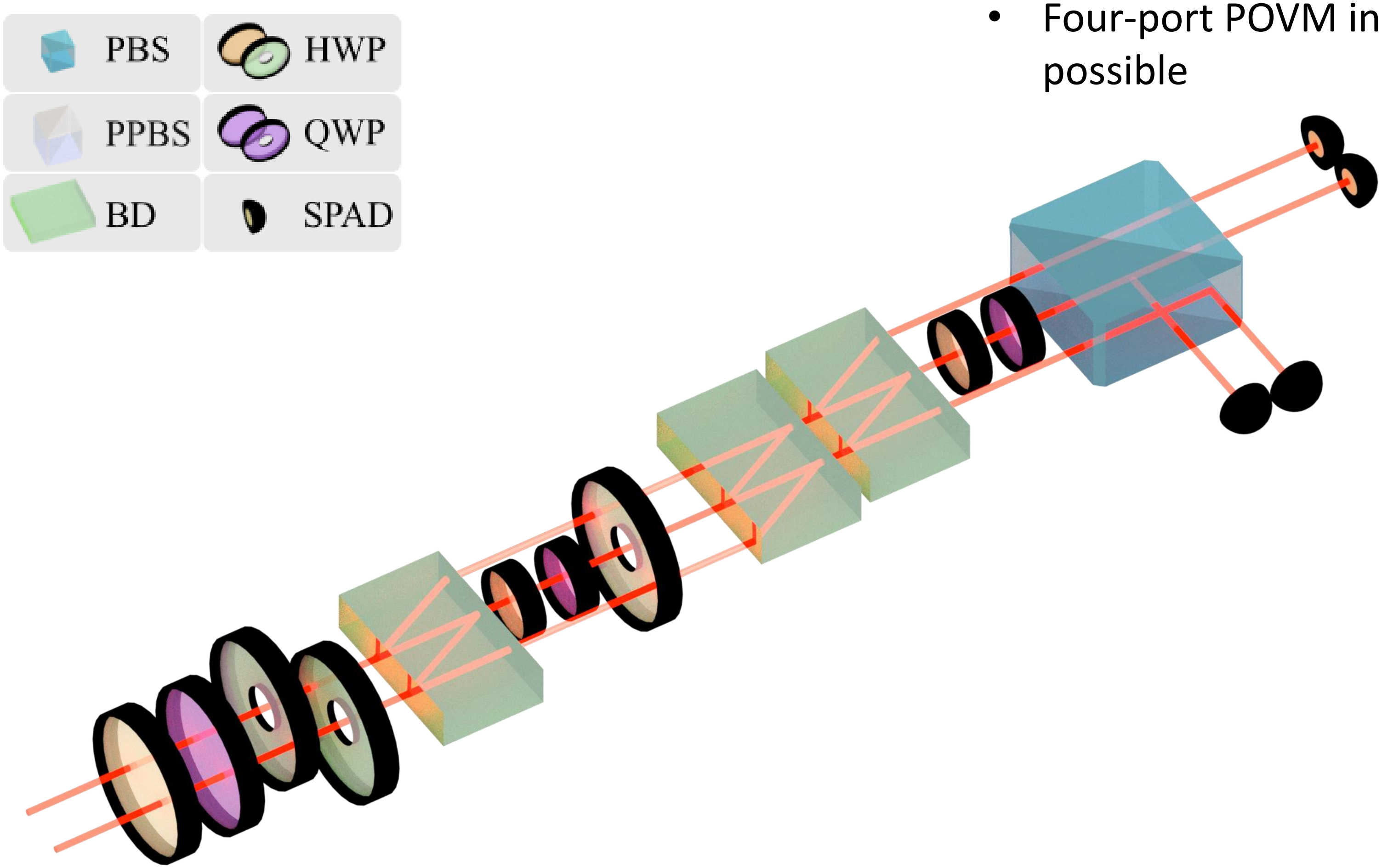
Detection



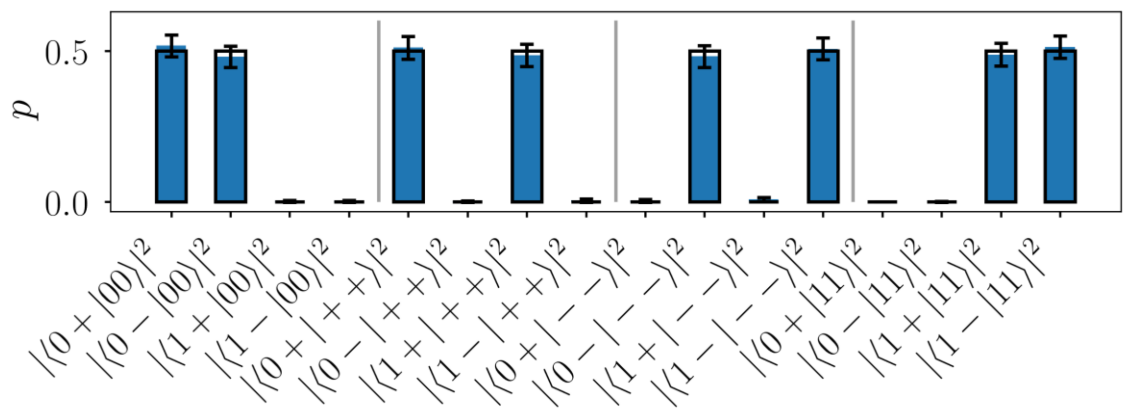
- Inverse to a preparation
- Photon-counting using SPAD
- Sequential measurement
- Four-port POVM in principle possible

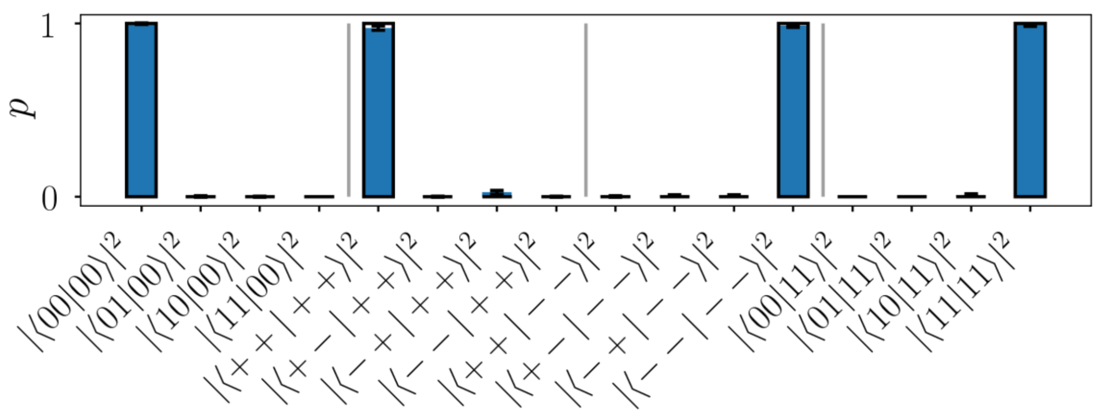
Detection

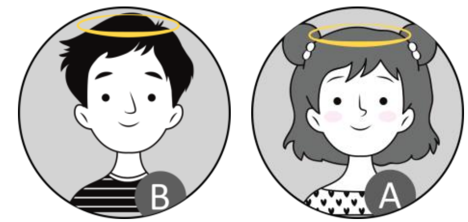
- Inverse to a preparation
- Photon-counting using SPAD
- Sequential measurement
- Four-port POVM in principle possible



Transfer protocol with honest parties

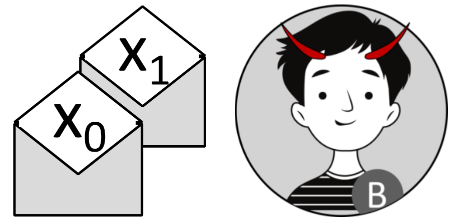


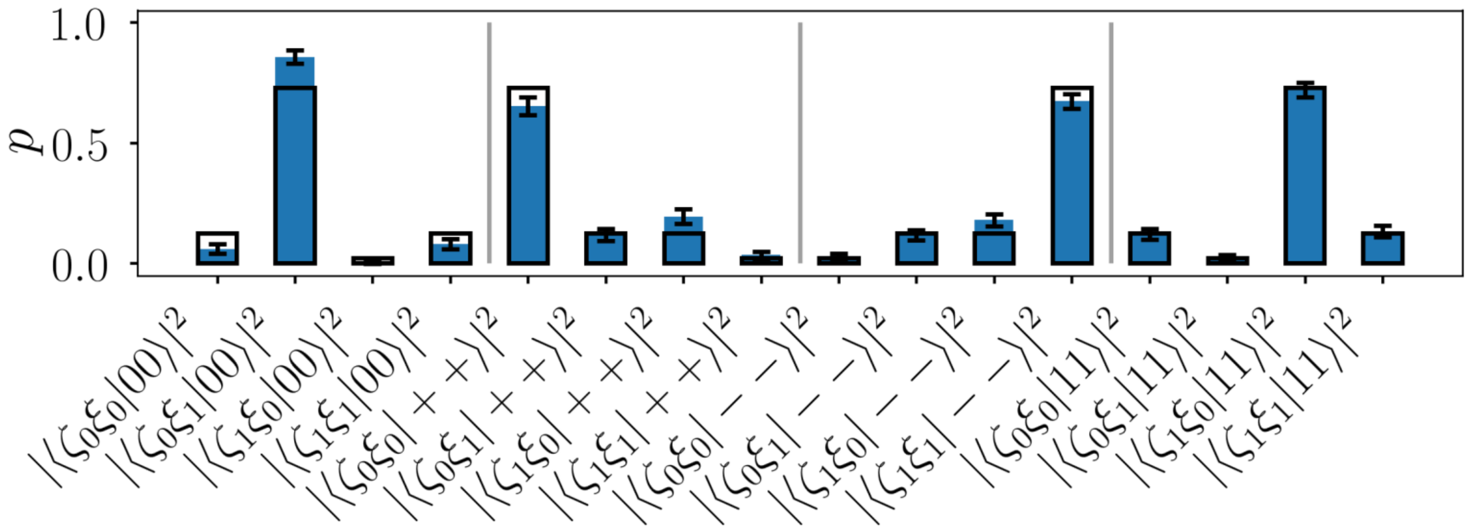




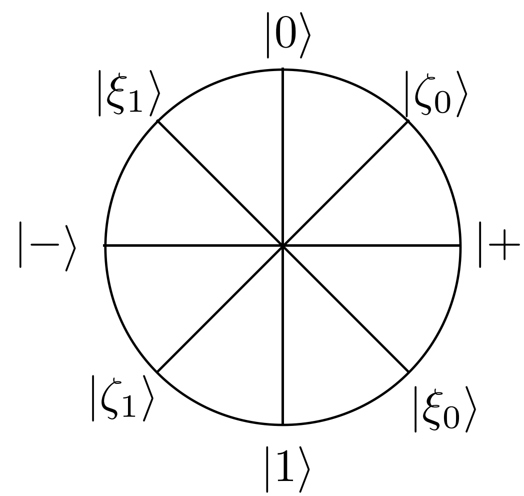
- $P_{corr.} = 0.9943(9)$
- $P_{abort} = 0.013(1)$

Cheating Bob



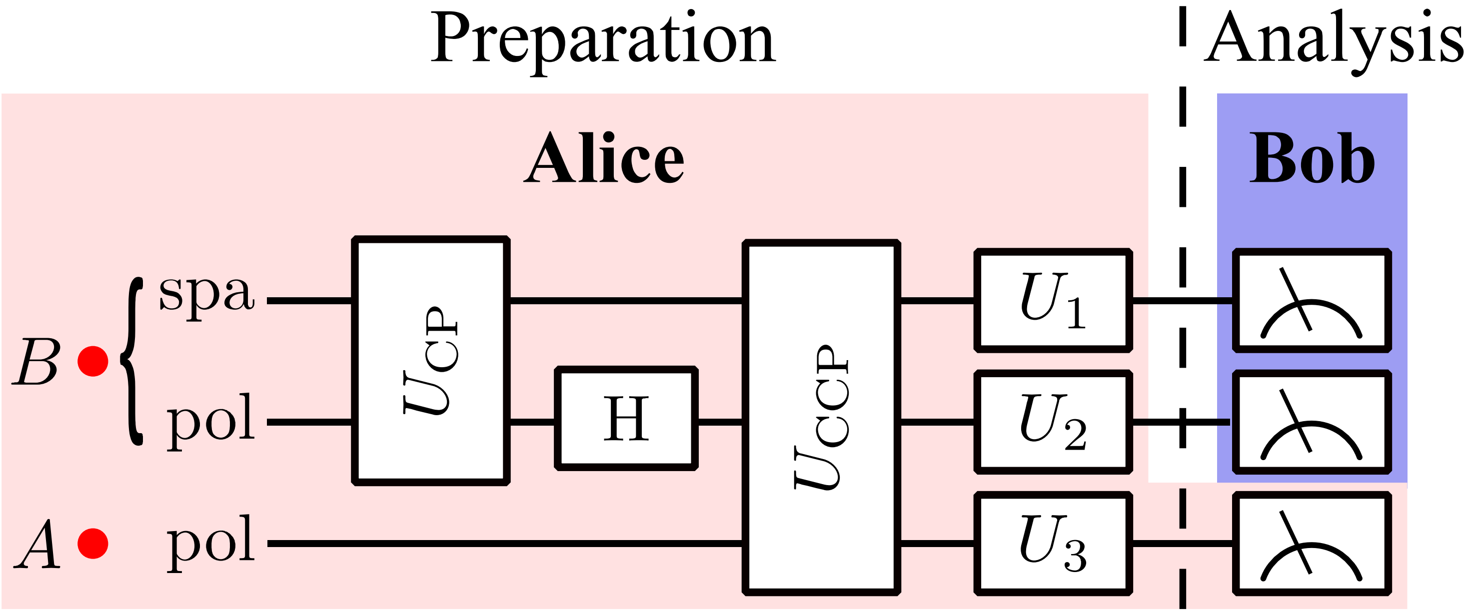


- Bob does minimum-error measurement
- $B_{OT} = \ 0.718(5)$
- Theoretical value: 0.729

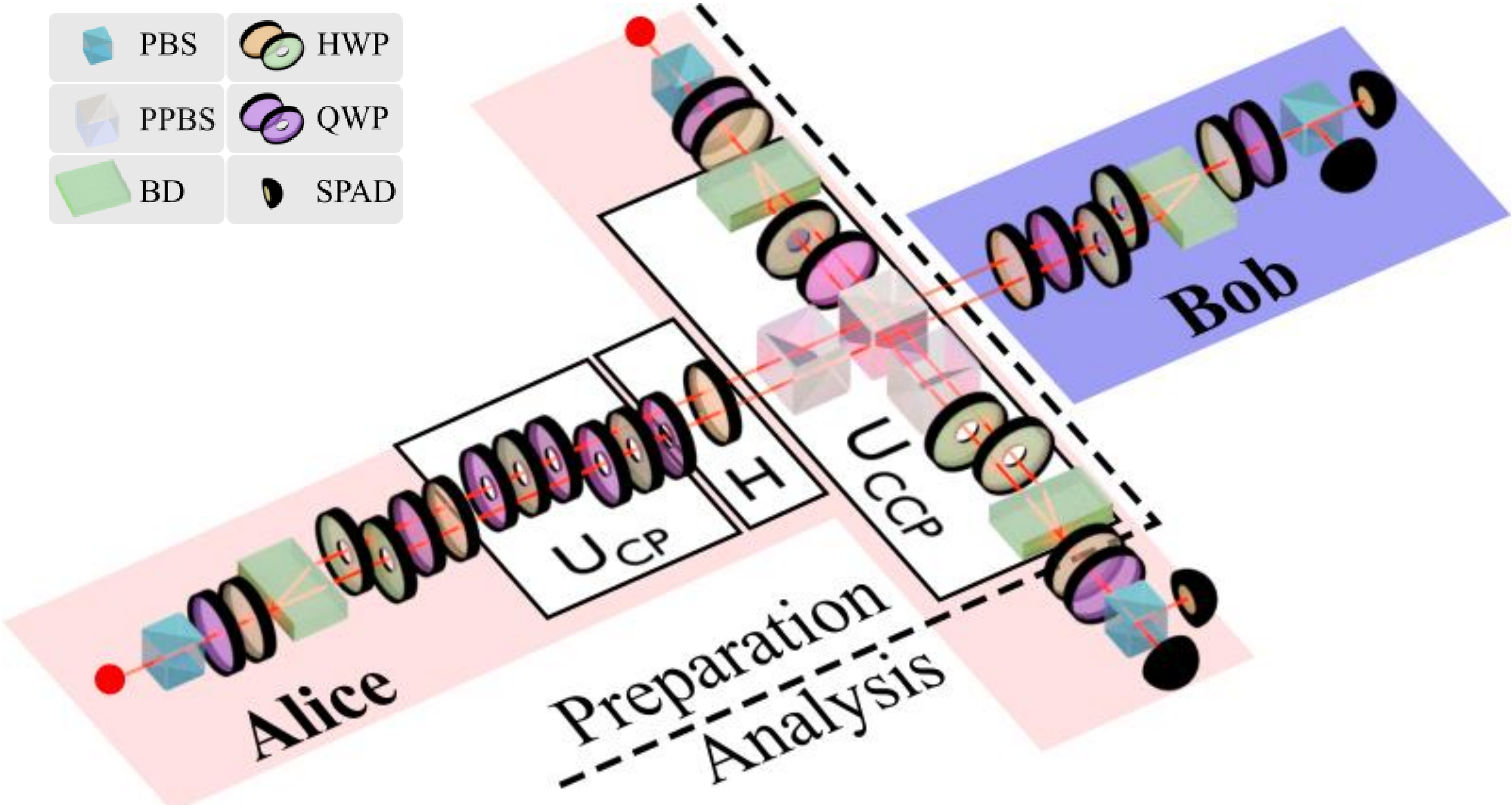


Cheating Alice

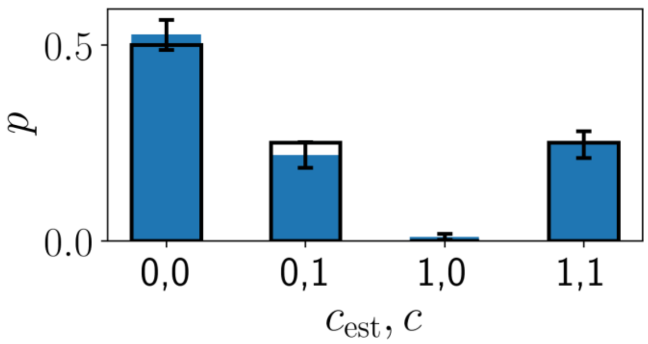
- Alice prepare $|\Sigma\rangle = \ (|00\rangle|0\rangle + |++\rangle|1\rangle\ )/\sqrt{2}$
- Conditional photonic quantum gates are used
- Alice measures on her qubit
- X basis for transfer, Z basis for testing
- Theoretically she can't be detected

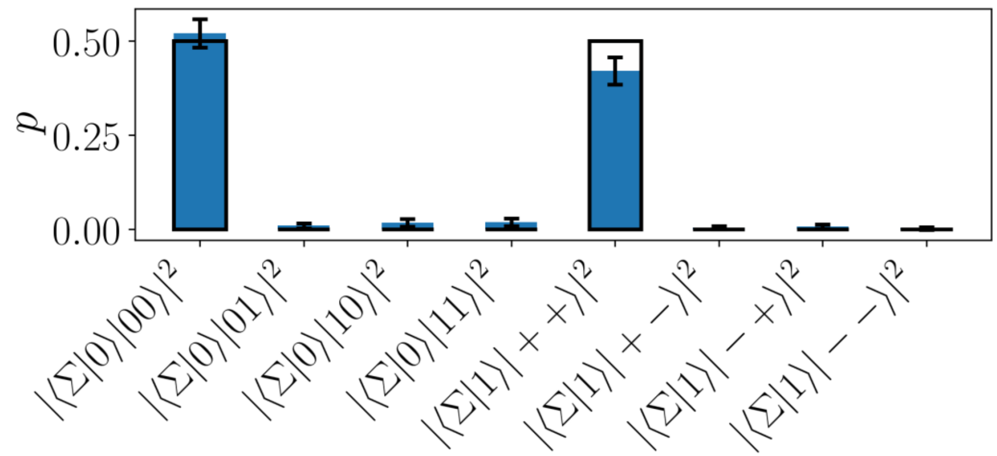


Cheating Alice



Cheating Alice

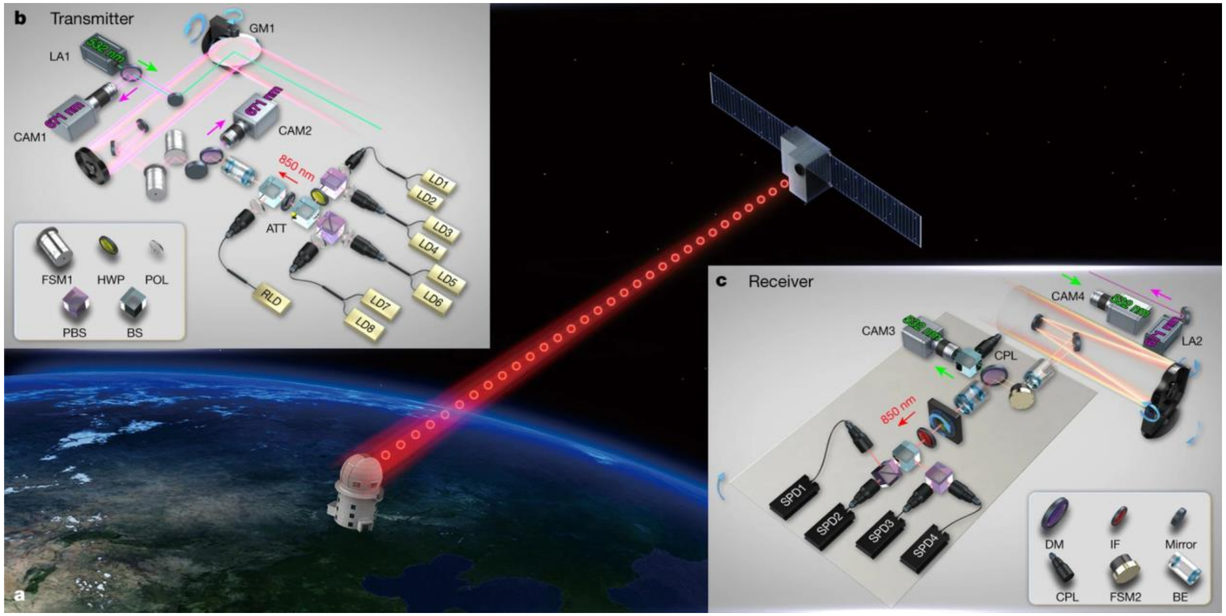




- $F_{\mathrm{exp|the}} = 0.921,\ P = 0.884$
- $A_{OT} = 0.77(1)$
- $p_{abort} = 0.059(6)$

Is the protocol practically feasible?

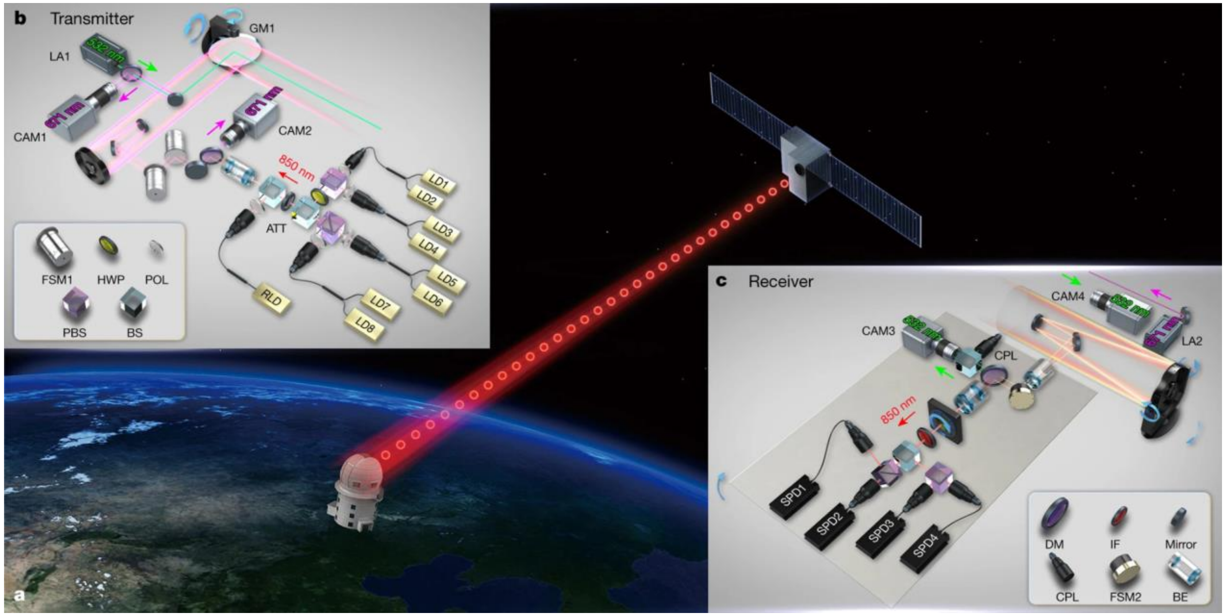
- Protocol requires the same elements as BB84 protocol.
- Instead of a single qubit, we transfer two qubits.
- Honest execution is therefore feasible. Quantum memory is not required.



- Liao, S. et al. Satellite-to-ground quantum key distribution, Nature 549, 43–47 (2017)
- A. Boaron et al., Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. 121, 190502 (2018)

How practical are the attacks?

- Bob's attack is feasible.
- Alice's attack is experimentally challenging.



- [Liao, S. et al. Satellite-to-ground quantum key distribution, Nature 549, 43–47 (2017)]
- [A. Boaron et al., Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. 121, 190502 (2018)]

Conclusion

- Concept of semi-random OT, equivalent to OT
- A feasible protocol for 1-2 OT, requiring only BB84 setup
- Proof-of-principle photonic experiment
- Symmetric pure states are not optimal in terms of security
- **Full paper: Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation,** arXiv:2007.04712

Acknowledgements

- EPSRC: EP/K022717/1, EP/M013472/1, EP/I007002/1
- Palacky University IGA-PrF-2020-009.

EPSRC

Engineering and Physical Sciences Research Council

Palacký University Olomouc

Drawings of Alice and Bob by freepik.com